August 2020

CYBERSECURITY

DHS and Selected Agencies Need to Address Shortcomings in Implementation of Network Monitoring Program

GAO Highlights

Highlights of GAO-20-598, a report to congressional requesters

Why GAO Did This Study

In 2013, DHS established the CDM program to strengthen the cybersecurity of government networks and systems by providing tools to agencies to continuously monitor their networks. The program, with estimated costs of about $10.9 billion, intends to provide capabilities for agencies to identify, prioritize, and mitigate cybersecurity vulnerabilities.

GAO was asked to review agencies' continuous monitoring practices. This report (1) examines the extent to which selected agencies have effectively implemented key CDM program requirements and (2) describes challenges agencies identified in implementing the requirements and steps DHS has taken to address these challenges.

GAO selected three agencies based on reported acquisition of CDM tools. GAO evaluated the agencies' implementation of CDM asset management capabilities, conducted semi-structured interviews with agency officials, and examined DHS actions.

What GAO Recommends

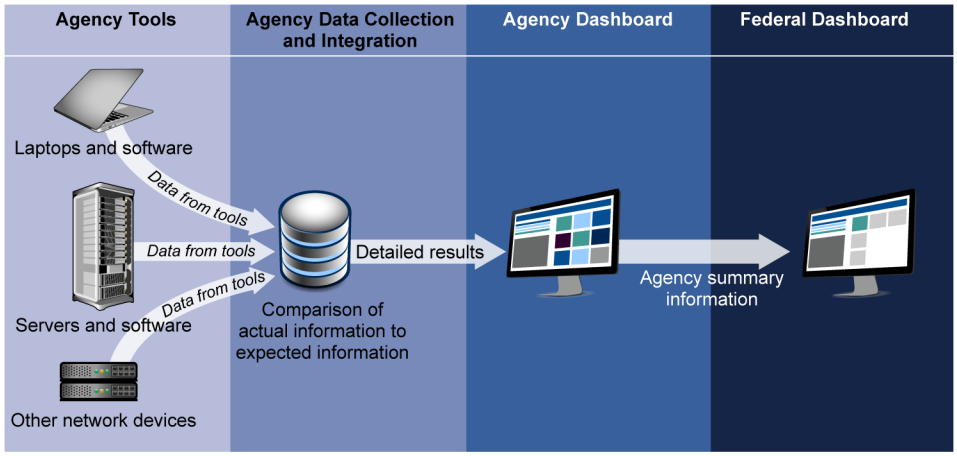
GAO is making six recommendations to DHS, including to ensure that contractors provide unique hardware identifiers; and nine recommendations to the three selected agencies, including to compare configurations to benchmarks. DHS and the selected agencies concurred with the recommendations.

View GAO-20-598. For more information, contact Vijay A. D'Souza at (202) 512-6240 or dsouzav@gao.gov.

What GAO Found

Selected agencies—the Federal Aviation Administration, Indian Health Services, and Small Business Administration—had generally deployed tools intended to provide cybersecurity data to support the Department of Homeland Security's (DHS) Continuous Diagnostics and Mitigation (CDM) program. As depicted in the figure, the program relies on automated tools to identify hardware and software residing on agency networks. This information is aggregated and compared to expected outcomes, such as whether actual device configuration settings meet federal benchmarks. The information is then displayed on an agency dashboard and federal dashboard.

Continuous Diagnostics and Mitigation Program Data Flow from Agencies to the Federal Dashboard



Source: GAO analysis of Department of Homeland Security data. | GAO-20-598

However, while agencies reported that the program improved their network awareness, none of the three agencies had effectively implemented all key CDM program requirements. For example, the three agencies had not fully implemented requirements for managing their hardware. This was due in part to contractors, who install and troubleshoot the tools, not always providing unique identifying information. Accordingly, CDM tools did not provide an accurate count of the hardware on their networks. In addition, although most agencies implemented requirements for managing software, they were not consistently comparing configuration settings on their networks to federal core benchmarks intended to maintain a standard level of security.

The agencies identified various challenges to implementing the program, including overcoming resource limitations and not being able to resolve problems directly with contractors. DHS had taken numerous steps to help manage these challenges, including tracking risks of insufficient resources, providing forums for agencies to raise concerns, and allowing agencies to provide feedback to DHS on contractor performance.